PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-123172
(43)Date of publication of application : 26.04.2002

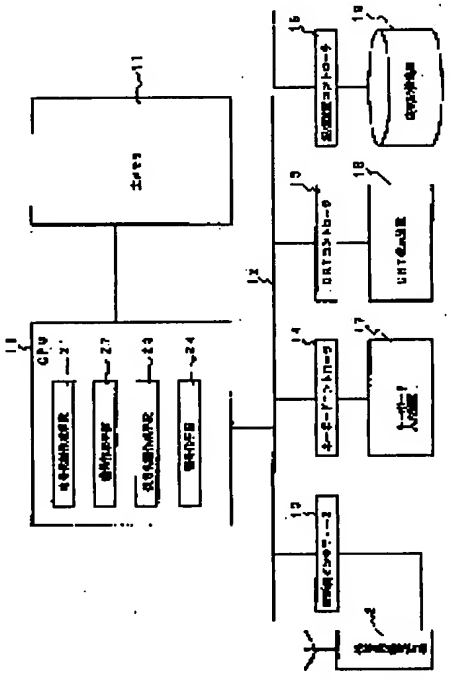
(51)Int.Cl. G09C 1/00
G06F 1/00
H04L 9/32

(21)Application number : 2000-315105
(22)Date of filing : 16.10.2000

(71)Applicant : TOSHIBA INFORMATION SYSTEMS (JAPAN) CORP
(72)Inventor : OGISHI NOBUYUKI

(54) ENCRYPTION APPARATUS, DECRYPTION APPARATUS, INFORMATION MANAGEMENT SYSTEM AND LOCKING SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To prohibit the decryption of encrypted information in places exclusive of a specific place.
SOLUTION: This apparatus includes a keyboard input device 17 for inputting information for forming an encryption key into which position information of a prescribed point is included, an encryption key forming means 21 for forming an encryption key from the information for forming the encryption key, a cipher forming means 22 for encrypting the information to be kept secret by using the formed encryption key, a portable wireless telephone 2 for receiving the position information of a present point from a position information notifying device, a decryption key forming means 23 for forming a decryption key by using the received position information and a decryption means 24 for decrypting the ciphertext formed by the cipher forming means 22 by using the formed decryption key.



LEGAL STATUS

[Date of request for examination] 16.10.2000
[Date of sending the examiner's decision of rejection] 27.01.2004
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's

decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－123172
（P2002－123172A）
(43)公開日　平成14年４月26日(2002.4.26)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)	
G09C	1/00	610	G09C	1/00	610Z	5B076
G06F	1/00		G06F	9/06	660Z	5J104
H04L	9/32		H04L	9/00	675A	

審査請求 有　請求項の数８ ＯＬ （全 ９ 頁）

(21)出願番号　特願2000－315105(P2000－315105)

(22)出願日　平成12年10月16日(2000.10.16)

(71)出願人　391016358
東芝情報システム株式会社
神奈川県川崎市川崎区日進町７番地１

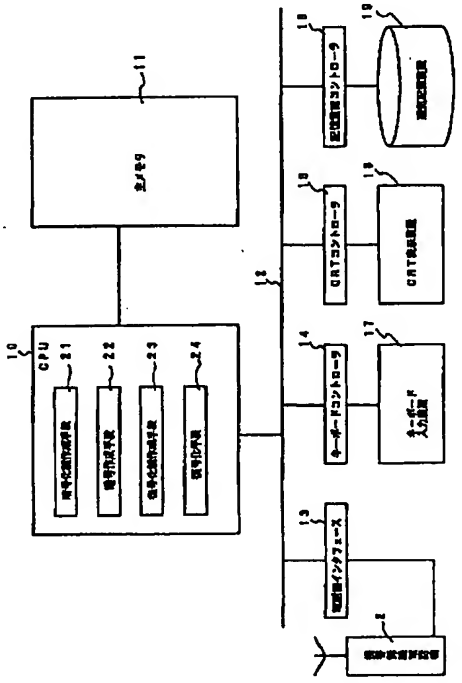
(72)発明者　大岸　伸之
神奈川県川崎市日進町７番地１　東芝情報システム株式会社内

(74)代理人　100074147
弁理士　本田　崇

Ｆターム(参考)　5B076 FA01 FA15 FA19
5J104 AA07 EA23 JA03 KA02 KA04
KA20 KA21 NA02 PA02

(54)【発明の名称】　暗号化装置、復号化装置、情報管理システム及び施錠システム

(57)【要約】
【課題】　特定の場所以外においては暗号化された情報を復号化できなくする。
【解決手段】　所定地点の位置情報が含まれた暗号化鍵作成用情報を入力するためのキーボード入力装置１７と、上記暗号化鍵作成用情報から暗号化鍵を作成する暗号化鍵作成手段２１と、作成された暗号化鍵を用いて秘匿すべき情報を暗号化する暗号作成手段２２と、現在地点の位置情報を位置情報通知装置から受信するための携帯無線電話機２と、受信した位置情報を用いて復号化鍵を作成する復号化鍵作成手段２３と、作成された復号化鍵を用いて前記暗号作成手段２２により作成された暗号文を復号化する復号化手段２４とを具備する。



前記入力部から位置情報と他の情報が暗号化鍵を作成する情報として入力されることを特徴とする。これによって、位置情報と他の情報から暗号化鍵が作成され、所定地点において位置情報を得て且つ上記他の情報から復号化鍵を作成した場合以外に暗号化された情報を解読できないようにできる。

【０００８】本発明の請求項３に記載の暗号化装置では、前記暗号化鍵作成手段は、位置情報に対し前記他の情報に基づくビットシフトをかけて暗号化鍵を作成することを特徴とする。これにより、暗号化された情報の解読をより困難にできる。

【０００９】本発明の請求項４に記載の復号化装置は、現在地点の位置情報を位置情報通知装置から受信するための受信機と、前記受信機が受信した位置情報を用いて復号化鍵を作成する復号化鍵作成手段と、この復号化鍵作成手段により作成された復号化鍵を用いて暗号文の復号化を行う復号化手段とを具備することを特徴とする。これにより、受信機が受信した現在地点の位置情報から復号化鍵が作成され、この現在地点の位置情報を用いて暗号化鍵を作成し暗号化した情報を適切に解読することができる。

【００１０】本発明の請求項５に記載の復号化装置は、復号化鍵を作成するための前記位置情報以外の他の情報を入力する入力部を具備し、前記復号化鍵作成手段は前記入力部から入力された他の情報と前記位置情報を用いて復号化鍵を作成することを特徴とする。これにより、受信機が受信した現在地点の位置情報と他の情報とから復号化鍵が作成され、この現在地点の位置情報及び他の情報を用いて暗号化鍵を作成し暗号化した情報を適切に解読することができる。

【００１１】本発明の請求項６に記載の情報管理システムは、所定地点の位置情報が含まれた暗号化鍵作成用情報を入力するための入力部と、この入力部から入力される暗号化鍵作成用情報から暗号化鍵を作成する暗号化鍵作成手段と、この暗号化鍵作成手段により作成される暗号化鍵を用いて秘匿すべき情報を暗号化する暗号作成手段と、現在地点の位置情報を位置情報通知装置から受信するための受信機と、前記受信機が受信した位置情報を用いて復号化鍵を作成する復号化鍵作成手段と、この復号化鍵作成手段により作成された復号化鍵を用いて前記暗号作成手段により作成された暗号文を復号化する復号化手段と、この復号化手段により復号化された情報を提供する情報提供手段とを具備することを特徴とする。これにより、受信機が受信した現在地点の位置情報から復号化鍵が作成され、この現在地点の位置情報を用いて暗号化鍵を作成し暗号化した情報を適切に解読することができる。

【００１２】本発明の請求項７に記載の施錠システムは、所定地点の位置情報が含まれた鍵作成用情報を入力するための入力部と、この入力部から入力される鍵作成用情報に基づき鍵情報の作成を行う第１の鍵情報作成手段と、前記鍵情報作成手段により作成された鍵情報を、開閉部分に取り付けられた錠の開閉制御の鍵とする制御手段とを具備することを特徴とする。これにより、所定地点が分からない限り施錠をはずすことができない施錠システムを提供できる。

【００１３】本発明の請求項８に記載の施錠システムは、現在地点の位置情報を位置情報通知装置から受信するための受信機と、前記受信機により受信された位置情報を用いて鍵情報を作成する第２の鍵情報作成手段とを具備し、前記制御手段は、前記第２の鍵情報作成手段により作成された鍵情報が前記第１の鍵情報作成手段により作成された鍵情報と一致する場合に、施錠を開放することを特徴とする。これにより、受信機が受信した現在地点の位置情報から鍵情報が作成され、この現在地点の位置情報を用いて施錠した錠を適切にはずすことができる。

【００１４】

【発明の実施の形態】以下添付図面を参照して本発明に係る暗号化装置、復号化装置、情報管理システム及び施錠システムを説明する。図１には、暗号化装置と復号化装置を備える情報管理システムの構成図が示されている。この情報管理システムは、図２に示されるように、ＧＰＳ（Global Positioning System ）の衛星１などの位置情報通知装置から現在地点の位置情報を受信する受信機である携帯無線電話機２をパーソナルコンピュータやオフィスコンピュータ等の情報処理装置３に接続して構成したシステムである。上記位置情報通知装置としては、ＰＨＳ位置情報システムなども適用可能である。

【００１５】図１に示すように、上記情報管理システムの情報処理装置３は、ＣＰＵ１０が主メモリ１１内のプログラムやデータを用いて各部を制御するシステムである。ＣＰＵ１０には、バス１２を介して電話機インタフェース１３、キーボードコントローラ１４、ＣＲＴコントローラ１５、記憶装置コントローラ１６が接続されている。

【００１６】電話機インタフェース１３には携帯無線電話機２が接続され、キーボードコントローラ１４にはキーボード入力装置１７が接続され、ＣＲＴコントローラ１５にはＣＲＴ表示装置１８、記憶装置コントローラ１６には磁気記憶装置１９が接続されている。勿論、これらのものは、入力、出力及び記憶の装置の例示に過ぎない。

【００１７】ＣＰＵ１０は、主メモリ１１内のプログラムを用いて暗号化鍵作成手段２１、暗号作成手段２２、復号化鍵作成手段２３、復号化手段２４として動作する。

【００１８】上記において、暗号化鍵作成手段２１は、携帯無線電話機２またはキーボード入力装置（入力部）から入力される暗号化鍵作成用情報から暗号化鍵を作成

作成される場合には、復号化鍵も図６により説明した手法により作成され、暗号化鍵が図７（または、図８）により説明した手法により作成される場合には、復号化鍵も図７（または、図８）により説明した手法により作成される。

【００３４】次にＣＰＵ１０は、磁気記憶装置１９から既に指示されている暗号化された対象データ（ファイル）を読み出し、上記ステップＳ１２において作成した復号化鍵を用いて、上記暗号化されたデータを平文に戻す解読処理をトライする（Ｓ１３（復号化手段２４））。このとき、ステップＳ１１において既に入力された位置情報等が暗号化鍵作成の際に用いた位置情報等と一致するか否かによって（Ｓ１４）、ステップＳ１５またはステップＳ１６が実行される。

【００３５】即ち、既にステップＳ１１において入力された位置情報等が暗号化鍵作成の際に用いた位置情報等と一致する場合（ステップＳ１４においてＹＥＳへ分岐する場合）には、当然に既に作成されている暗号化鍵と復号化鍵が一致することになるから、暗号化されたデータを平文に戻す解読処理を行うことができ、これが実行されることになり（Ｓ１４の前半（復号化手段２４））、斯して得られた平文化されたファイルをＣＲＴ表示装置１８へ表示するなどする（Ｓ１４の後半（情報提供手段））。

【００３６】上記に対して、既にステップＳ１１において入力された位置情報等が暗号化鍵作成の際に用いた位置情報等と不一致であると（ステップＳ１４においてＮＯへ分岐すると）、復号化処理が失敗に終わり、エラーである旨をＣＲＴ表示装置１８へ表示する（Ｓ１６）。このように、本実施の形態によれば、情報管理システムが位置している現在位置が所定の位置でないときには、携帯無線電話機２から得られる位置情報が暗号化鍵作成に用いたものと異なり、作成された復号化鍵によっては暗号化された対象データの復号化ができず、適正な場所以外へシステムを持ち運ぶと情報の秘匿化が確実になされることになる。

【００３７】また、時刻情報を暗号化鍵の作成に用い、時刻情報を情報管理システムのタイマから得るようにすると、暗号化の際に設定した時刻でない場合には、暗号化された対象データの復号化ができず、適正な時刻以外の時刻において情報の秘匿化を確実に行える。

【００３８】次に、本発明に係る施錠システムを説明する。図５に示す施錠システムは、ソレノイド駆動による錠３１が、金庫や扉、更に箱の蓋などの開閉部に取り付けられている。錠３１のアクチュエータがドライバを含む制御手段３２の制御により矢印Ａのように左右に動き、施錠状態と解錠状態を実現する。

【００３９】図５の施錠システムには、テンキー或いはテンキーと必要な文字キー等が設けられた入力部３８と、マイクロプロセッサ等のコンピュータ部３０とが備えられている。

【００４０】コンピュータ部３０には、制御手段３２、第１の鍵情報作成手段３３、第２の鍵情報作成手段３４が設けられ、第１の鍵情報作成手段３３と第２の鍵情報作成手段３４には携帯無線電話機２を接続する端子３５が接続されている。

【００４１】制御手段３２、第１の鍵情報作成手段３３は、入力部３８から入力される鍵作成用情報に基づき鍵情報の作成を行うものである。第２の鍵情報作成手段３４は、受信機である携帯無線電話機２により受信された位置情報を用いて鍵情報を作成するものである。制御手段３２は、第１の鍵情報作成手段３３により作成された鍵情報を、錠３１の開閉制御の鍵とすると共に、第２の鍵情報作成手段３４により作成された鍵情報が第１の鍵情報作成手段３３により作成された鍵情報と一致する場合に、錠３１の施錠を開放するように機能する。

【００４２】以上のように構成された施錠システムの動作を説明する。この動作は、図３、図４のフローチャートの括弧内に記述されているものである。鍵３１の施錠を行う場合には、入力部３８から施錠の指示と鍵情報作成の指示とを入力する。これにより、制御手段３２は第１の鍵情報作成手段３３に鍵情報作成の指示を与える。これを受けて、第１の鍵情報作成手段３３は、携帯無線電話機２から位置情報を得て（必要であれば、入力部３８から時刻情報やパスワードを得て）、図６～図８を用いて説明した手法のいずれか所定の手法により鍵情報を作成し、制御手段３２へ送る。

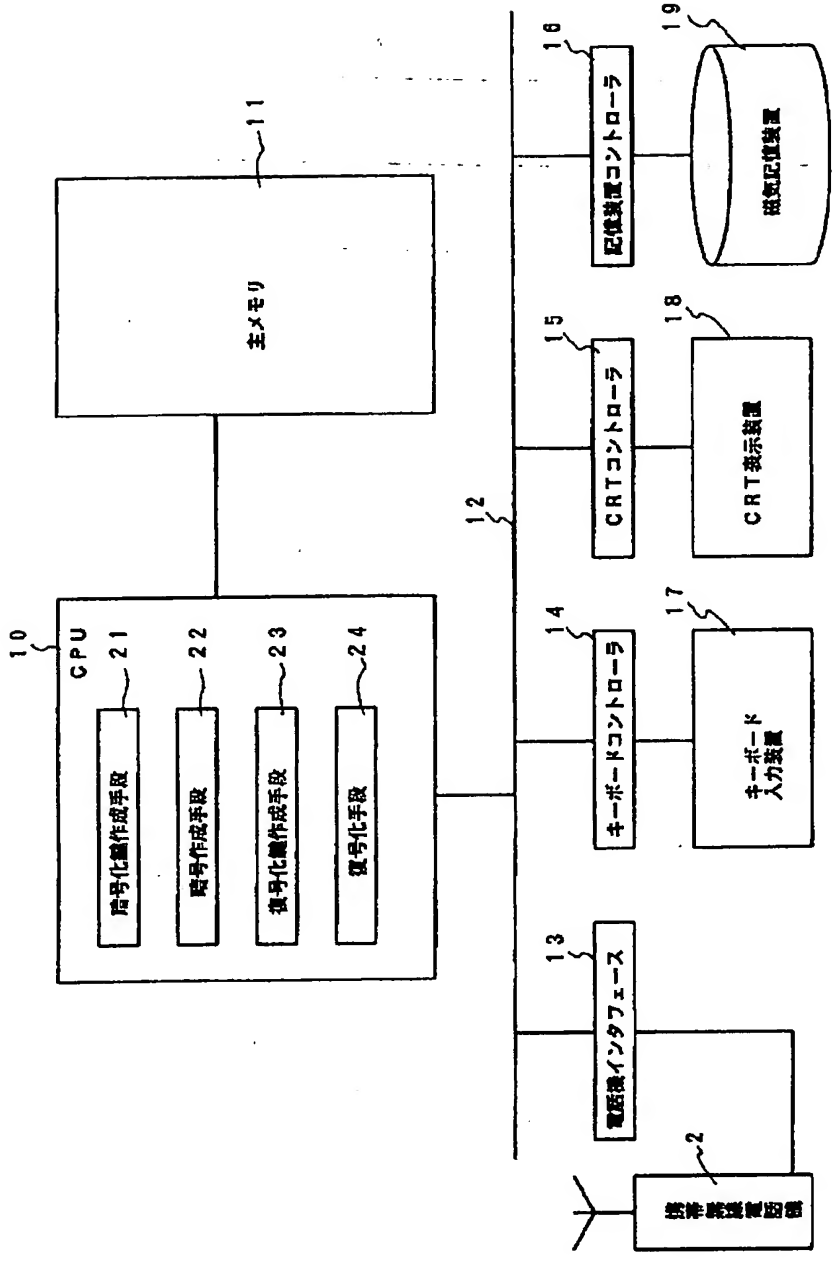
【００４３】制御手段３２は、上記鍵情報を保持し、対応して錠３１を施錠する。この施錠された錠を持つ金庫や箱は運搬され、この施錠を解くべき場所に置かれる。施錠を解く場合には、携帯無線電話機２を端子３５に接続し、入力部３８から施錠の解除の指示を入力する。

【００４４】これにより、制御手段３２は第２の鍵情報作成手段３４に鍵情報作成の指示を与える。これにより、第２の鍵情報作成手段３４は、携帯無線電話機２から位置情報を得て（必要であれば、入力部３８から時刻情報やパスワードを得て）、上記所定の手法により鍵情報を作成し、制御手段３２へ送る。

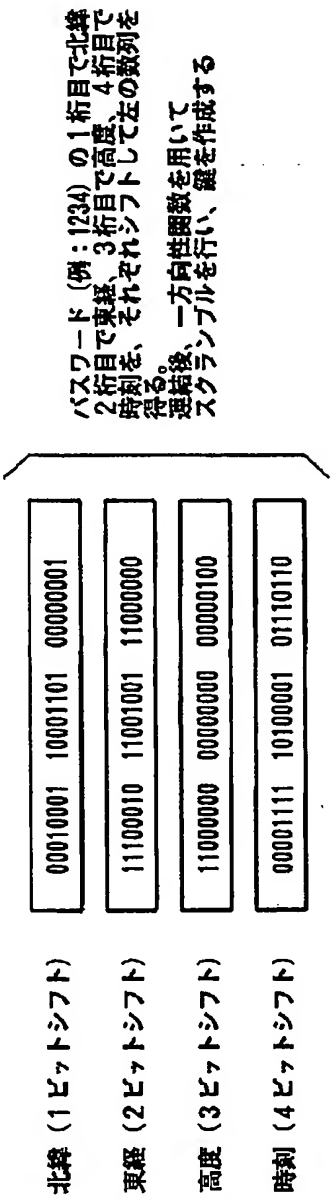
【００４５】制御手段３２は、鍵情報を用いて錠３１の解錠をトライする。既に第１の鍵情報作成手段３３により鍵情報が作成されたときに入力された位置情報等が、第２の鍵情報作成手段３４により鍵情報を作成する際の位置情報等と一致する場合（ステップＳ１４においてＹＥＳへ分岐する場合）には、当然に２つの鍵情報が一致するかことになるから、解錠が実行され、不一致のときには施錠のままとする。これにより、金庫や箱の蓋等は、所定の場所にない場合には解錠することができず、例えば、現金輸送車などに適用すると特定の場所に駐車していない限り、扉が開くことを防止でき防犯に役立てることができる。

ータ部
３１　鍵
段
３２　制御手
３３　第１の鍵情報作成手段
鍵情報作成手段
３８　入力部
３４　第２の

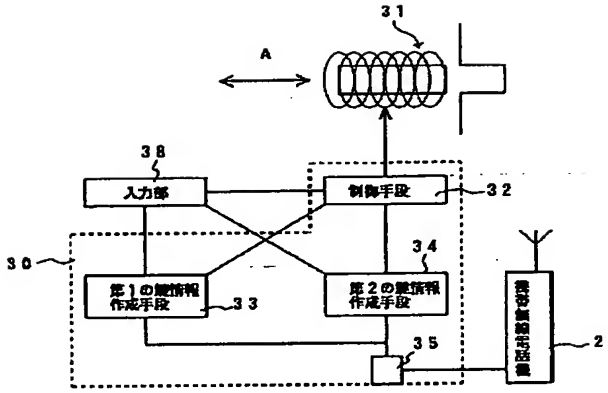
【図１】



【図８】



【図５】



【図６】

北緯	00100011 00011010 00000010
東経	10001011 00100111 00000011
高度	00000000 00000000 00100110

北緯、東経、高度のみの数列を
連結後、一方向性関数を用いて
スクランブルを行い、鍵を作成する

【図７】

北緯	00100011 00011010 00000010
東経	10001011 00100111 00000011
高度	00000000 00000000 00100110
時刻	01111101 00001011 10110000

北緯、東経、高度に時刻情報を付加し、
連結後、一方向性関数を用いて
スクランブルを行い、鍵を作成する